**INFORME Nº 005 - 2011- USI**

**INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE**

## 1. Nombre del Área

El área asignada de la evaluación técnica para la adquisición de licencias de herramienta de administración de riesgos y auditoría interna es la Unidad de Seguridad Informática de la Caja Metropolitana.

## 2. Nombre y Cargo del Responsable de la Evaluación

Los analistas responsables de la evaluación son los señores Jhon Alvarado y Luis Espinoza.

## 3. Fecha

La fecha del presente informe es del 05 de setiembre de 2011.

## 4. Justificación

La SBS ha emitido regulaciones relacionado con la Gestión Integral de Riesgos, usando como metodología base el COSO-ERM. En este marco, la resolución SBS Nº 037-2008 en el artículo 22º establece que Auditoría Interna - UAI debe "vigilar la adecuación de la Gestión Integral de Riesgos", asimismo, la resolución SBS Nº 2116-2009 "Reglamento de Gestión de Riesgo Operacional", en el artículo 17º establece que la UAI deberá "evaluar el cumplimiento de los procedimientos utilizados para la gestión de Riesgo Operacional". Para tal efecto, la UAI debe adecuarse a una Auditoría basada en Riesgos, necesitando para ello, del soporte de una herramienta que le permita registrar el resultado de la evaluación de todo el ciclo de Gestión de Riesgos (Identificación, documentación, medición, control, tratamiento y monitoreo de los riesgos) a lo largo de toda la institución, así como del registro de Eventos de Pérdida detectados por la UAI.

Esta herramienta debe de ser capaz de soportar los siguientes procesos:

- ✓ Enfoque basado en la gestión de Riesgos.
- ✓ Procedimientos de Auditoría aplicados por Examen: planeación, ejecución y administración de papeles de trabajo, emisión de hallazgos, informe final y seguimiento de observaciones
- ✓ Visibilidad y colaboración amplia y universal vía la web.
- ✓ Flexibilidad en la forma de personalización por parte del usuario.

Actualmente, la UAI utiliza la herramienta Pro Audi Advisor 5.0 (cuyas 3 licencias vencieron en agosto del 2011), que utiliza para registrar los Riesgos y Controles definidos en la Matriz de Riesgos de la Caja, así como para el registro de las observaciones y recomendaciones por Examen y el seguimiento de su implementación, sin embargo, no permite el registro de la evaluación de todo el ciclo de Gestión de Riesgos ni el registro de eventos de pérdida.

## 5. Alternativas

**Los Software de Auditoria:** Son programas utilizados para procesar grandes cantidades de datos generados por la contabilidad de una organización, pueden ser:

Programas en paquete, programas escritos para un propósito específico y programas de utilería.

Los principales pasos para tomar en cuenta en la identificación del aplicativo serian:

- ✓ Fijar el objetivo de la aplicación.
- ✓ Determinar el contenido y accesibilidad de los archivos de la entidad.
- ✓ Definir los tipos de transacción que van a ser probados.
- ✓ Definir los procedimientos que se realizarán en los datos.
- ✓ Definir los requerimientos de datos de salida.
- ✓ Identificar al personal de auditoría y de computación que pueda participar en el diseño y aplicación.
- ✓ Refinar los estimados de costos y beneficios.
- ✓ Asegurarse de que el uso del aplicativo está controlado y documentado en forma apropiada.
- ✓ Organizar las actividades administrativas, incluyendo las habilidades necesarias y las instalaciones de computación.
- ✓ Ejecutar la aplicación.
- ✓ Evaluar los resultados.

## 5.1 Características deseables de un software de auditoria

Se ha tomado en cuenta que el software de auditoría se tomara en cuenta las siguientes características:

***Características Generales***

El software de auditoría debe de tener:

- ✓ Manual de Usuario, Manual Técnico y Material de Capacitación.
- ✓ Opciones de copiar o exportar cualquier documento como papeles de trabajo a aplicaciones ofimáticas como Word, Excel, Power Point y otros.
- ✓ Capacidad de acumular la información histórica, y además de poderla consultar por año.
- ✓ Capacidad de poder funcionar como un todo integrado entre las diferentes etapas y procesos de la Auditoria: Planeación; Administración de Riesgos; Ejecución y Administración de Papeles de Trabajo; Evaluación de Administración de TI; Análisis y Evaluación de Base de Datos; Emisión de Informes

***Características de Seguridad***

El software de auditoría debe de tener:

- ✓ Posibilidad de definir que usuarios puedan acceder al sistema.
- ✓ Administración de los permisos de las opciones a las que tiene derecho un usuario a ejecutar, consultar según su cargo y área a la que pertenezca.
- ✓ Opciones de incluir pistas de auditoría en procesos, control de cambios, lectura,
- ✓ escritura y modificación de parte de los usuarios.
- ✓ Copias de respaldo de la información mediante BACKUP en medios magnéticos/ópticos y COMPROBAR cómo recuperar los datos del Backup.

## 6. Análisis Técnico

Para este tipo de auditorías se manejan los siguientes puntos:

- ✓ Automatizar todos los aspectos de riesgos dentro de una herramienta dinámica.

- ✓ Base de datos de metodologías/técnicas de Análisis de Riesgos. Algunos ejemplos: Delphi; Análisis por Tablas; MAGERIT; NIST Risk Managment Guide; AS/NZS 4360:2004 Risk Managment.
- ✓ Opciones de realizar análisis de riesgo cualitativo, cuantitativo y mixto.
- ✓ Definición de parámetros para el análisis cuantitativo del riesgo.
- ✓ Tener un repositorio central y compartido que puede ser accedido por auditores internos y personal externo al área de auditoría que previamente haya sido debidamente autorizado.
- ✓ Monitorear y dar seguimiento a la información de las auditorias y al cumplimiento de las recomendaciones.
- ✓ Presentación de Registro histórico de auditorías por temas (Consolidación de estudios a través del tiempo).
- ✓ Rastrear el rendimiento de los indicadores claves de riesgo.
- ✓ Contar con una clara imagen de la información del riesgo en cualquier nivel de la
- ✓ organización; a través de matrices de riesgos y otros gráficos.
- ✓ Proveer a la organización un sistema de administración de riesgos, con indicadores de riesgo, eventos de riesgo y tratamientos de riesgo.
- ✓ Generar reportes los cuales estén completamente integrados con Microsoft Office.

Del benchmarking realizado se han identificado los siguientes software disponibles en el mercado y que cumplen con las características generales y de seguridad:

**RISK2K – Pilar – Chinchón**

***Resultado:***

Estos programas permiten implementar los conceptos y procesos propuestos por la metodología MAGERIT para el análisis y gestión de riesgos. Los objetivos básicos del MAGERIT son estudiar los riesgos y recomendar contramedidas, esto se consigue cargando la base de datos información como: Grupos de activos, Amenazas, Grupos de amenazas, Tipos de amenazas, Funciones de salvaguarda, Tipos de funciones de salvaguarda, Mecanismos de Salvaguarda.

La metodología MAGERIT está compuesta por: Guía de Aproximación, Guía de Procedimientos, Guía Técnica, Guía para desarrolladores de aplicaciones, Guía para responsables del dominio protegible, Referencia de normas legales y Técnicas.

**Enterprise Risk Assessor (ERA)**

***Resultado:***

Es una versión mejorada del Pro Audit Advisor que además de los procesos de auditoría, permite la gestión y control del riesgo, proporciona: Un sistema consistente de gestión de riesgos; Identificación específica de riesgos para la estrategia y contexto organizacional; Gestión para los planes de acción, y monitoreo mediante una base de datos;

Asimismo, permite la evaluación de riesgos, controles y amenazas semi-cuantitativas, a través de análisis de consecuencias; Gráficos de análisis; Reportes de alta calidad alineados a los requerimientos individuales de los negocios.

**Risk Assesment Program – RAP**

***Resultado:***

RAP es un programa de análisis de riesgos y contramedidas basándose en la técnica de Tablas en la que se identifican riesgos y se determina la probabilidad, impacto y en función a estos dos últimos se calcula el Nivel de

Riesgo Asociado. Las contramedidas se asignan de acuerdo al mayor Nivel de Riesgo que presenten los Activos de Información de la organización.

## 7. Conclusiones

Las conclusiones de la evaluación realizada son las siguientes:

- ✓ El tamaño y complejidad de las operaciones de la Caja Metropolitana, hacen necesario contar con una herramienta de permita optimizar los procesos de Auditoría en base a la gestión de Riesgos

- ✓ Es importante resaltar que personal de Auditoría Interna, está capacitado y familiarizado con las funcionalidades del Pro Audi Advisor, de allí que upgrade al softwareERA representa la herramienta más alineada a los procesos de la UAI, con tiempos menores de implementación y costos sólo de licenciamiento, evitando incurrir en costos de adquisición de la herramienta.

- ✓ Dada la importancia del uso de la herramienta de administración de riesgos y auditoría interna, se hace necesario el mantener una política de licenciamiento adecuada, que permita no sólo cubrir los requerimientos de este software, sino también reducir los costos financieros y operativos asociados.